The Amended Claims Distinguish Over the Applied References

Applicant has amended independent claim 1 to recite, in combination:

> 1. A method for establishing a secure communications session between a first computing device and a second computing device, the method comprising :
>
> retrieving a first random number at the first computing device;
>
> retrieving a second random number at the second computing device;
>
> retrieving at least one public-private key pair including a public key and a private key;
>
> sending a message from said second computing device to said first computing device, said message from said second computing device to said first computing device including said first random number and the public key of said at least one public-private key pair to thereby share at least said first random number with said first communication device, said message from said second computing device to said first computing device being encrypted with an encoded password;
>
> providing said encoded password to said first computing device;
>
> using said provided encoded password to decrypt said first message at said first computing device to obtain at least said first random number that said second computing device sent in said message from said second computing device to said first computing device;
>
> sending a message from said first computing device to said second computing device, said message from said first computing device to said second computing device including said second random number, said first computing device encrypting said message it sends to said second computing device;
>
> generating, at each of said first and second computing devices, a shared session key by combining said first random number and second random number that is now available to each of said first and second computing devices through said above-mentioned message exchanges; and
>
> using said shared session key to establish a secure private communication session between said first and second computing devices.

Applicant has similarly amended independent claim 154 to recite, in combination:

154. A method for establishing secure communication between a calling party and a called party, comprising:

generating, on demand at the called party, an asymmetric key pair including a public key and a private key;

transmitting, from said called party to said calling party, a first encrypted message including a first random number and said public key of said asymmetric key pair, said called party encrypting said first message with an encoded password known to both the calling party and the called party;

said calling party receiving and decrypting said first encrypted message using said encoded password to obtain said first random number and said public key;

said calling party transmitting, to said called party, a second encrypted message including a second random number, said calling party encrypting said second message with said public key of said asymmetric key pair;

said called party receiving and decrypting said second encrypted message to obtain said second random number;

said calling and called parties each independently applying said now-shared first and second random numbers to combining functions to thereby each independently generate a shared secret key; and

said calling and called parties encrypting further communications therebetween at least in part using said shared secret key.

Applicant respectfully submits that independent claims 1 and 154 as amended clearly patentably distinguish over the applied references. For example, none of the applied references teaches, in combination, the use of the password as claimed to provide authentication in the context of the particular claimed combinations. While the applied Bellovin et al. reference discloses use of a password as a key to produce a Data Encryption Standard (DES) encryption (column 5, lines 18-32; see Office Action at 4), Bellovin's use of a password is different from what applicant has claimed.

All outstanding issues have been addressed, and applicant believes the present application is in condition for allowance. Should any minor issues remain outstanding,

the Examiner is encouraged to contact the undersigned at the telephone number listed below.

The Commissioner is hereby authorized to charge any deficiency, or credit any overpayment, in the fee(s) filed, or asserted to be filed, or which should have been filed herewith (or with any paper hereafter filed in this application by this firm) to our Account No. 14-1140.

Respectfully submitted,

NIXON & VANDERHYE P.C.

By: /Robert W. Faris/
Robert W. Faris
Reg. No. 31,352

RWF:ejs
901 North Glebe Road, 11th Floor
Arlington, VA 22203-1808
Telephone: (703) 816-4000 / Facsimile: (703) 816-4100